

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application.
Claim 19 has been cancelled without prejudice or disclaimer.

Listing of Claims:

1. (Currently amended) A method of providing key management comprising:
- providing a server;
 - providing a client configured to be coupled to said server;
 - providing a trusted third party configured to be coupled to said client;
 - generating a trigger message at said server for triggering said key management;
 - generating a nonce at said server;
 - coupling said nonce with said trigger message;
 - allowing said server to initiate a key management session with said client;
 - utilizing said nonce coupled with said trigger message.
2. (Previously presented) The method as described in claim 1 wherein said allowing said server to initiate said key management session with said client comprises:
- conveying said trigger message and said nonce to said client.
3. (Original) The method as described in claim 2 and further comprising:
- receiving said trigger message and said nonce at said client;
 - generating a response message to said trigger message;
 - conveying said response message and a returned_nonce to said server.
4. (Original) The method as described in claim 3 and further comprising:
- predetermining an out-of-bounds value for said nonce to prevent an attacker from simulating a client initiated key management session;

checking said nonce to determine whether the value of said nonce is said out-of-bounds value.

5. (Original) The method as described in claim 3 and further comprising:
confirming the value of said returned_nonce at said server; and
conveying a reply message from said client to said server.

6. (Original) The method as described in claim 1 and further comprising:
receiving from said client a response message and a false_nonce at said server;

determining that said false_nonce is false;
disregarding said client response message.

B1
7. (Currently amended) A method of providing key management in a Kerberos based system, said method comprising:
providing a server;
providing a client configured to be coupled to said server;
providing a key distribution center configured to act as a trusted third party for said client and said server;
generating a nonce at said server;
generating a trigger message to trigger said key management;
conveying said trigger message and said nonce to said client;
coupling said trigger message with said nonce;
initiating a key management session by said server with said client by utilizing said nonce coupled with said trigger message.

8. (Previously presented) The method as described in claim 7 and further comprising:
conveying said trigger message and said nonce to said client.

9. (Original) The method as described in claim 8 and further comprising:
receiving said trigger message and said nonce at said client;
generating a response message to said trigger message;
conveying said response message and a returned_nonce to said server.

10. (Original) The method as described in claim 9 and further comprising:
confirming the value of said returned_nonce at said server; and then
continuing with said key management session.

31
11. (Original) The method as described in claim 7 and further comprising:
receiving at said server a response message and a false_nonce from said
client;
determining that said false_nonce does not match said nonce;
determining that said server did not initiate said key management session.

12. (Previously presented) A method of initiating a key management session
for a cable telephony adapter (CTA) and a Signaling Controller in an IP Telephony network, the
method comprising:

providing said Signaling Controller;
providing said CTA configured to be coupled to said Signaling Controller;
providing a key distribution center (KDC);
generating a trigger message at said Signaling Controller;
generating a nonce at said Signaling Controller;
coupling said nonce with said trigger message;
transmitting said nonce coupled with said trigger message to said CTA;
generating a response message to said trigger message;
using the value of said nonce as the value of a returned_nonce;
coupling said response message with said returned_nonce;

transmitting said returned_nonce and said response message to said Signaling Controller;
comparing said returned_nonce to said nonce;
transmitting an AP reply in reply to said response message;
transmitting an SA recovered message to said Signalling Controller.

13. (Original) A method of conveying a key from a server to a client, comprising:
generating a wakeup message at said server;
generating a server_nonce at said server;
conveying said wakeup message and said nonce to said client;
generating an AP request message at said client;
conveying a client_nonce and said AP request message to said server;
confirming that said client_nonce conveyed with said AP request message matches said server_nonce generated at said server;

14. (Original) A method of confirming that a message received by a server from a client was triggered by the server:
receiving an AP request message from said client;
receiving a client_nonce from said client wherein said client_nonce is associated with said AP request;
determining whether said client_nonce matches a nonce conveyed from said server.

15. (Original) The method as described in claim 14 and further comprising:
determining that said client_nonce does not match said nonce conveyed from said server; and
disregarding said AP request.

16. (Original) The method as described in claim 15 and further comprising:

awaiting at said client for a reply from said server to said AP request;
aborting said AP request session after a predetermined time period if no
reply is received from said server.

17. (Original) The method as described in claim 14 and further comprising:
determining that said client_nonce does match said nonce conveyed from
said server; and
generating an AP reply at said server to said AP request.

18. (Currently amended) A system for providing key management in a
Kerberos based system, said system comprising:
a server;
a client configured to be coupled to said server;
a key distribution center configured to act as a trusted third party for said
client and said server;
computer code coupled to said server operable to initiate a key
management session by said server with said client;
computer code coupled to said server operable to generate a nonce at said
server;
computer code coupled to said server operable to convey said trigger
message and said nonce to said client.

19. (Cancelled)

20. (Currently amended) The system as described in claim 18 ~~19~~ and further
comprising:
computer code coupled to said client operable to generate a response
message to said trigger message;

Appl. No. 09/668,426
Amdt. dated April 26, 2004
Reply to Office Action of April 8, 2004

PATENT

computer code coupled to said client operable to convey said response
message and a returned_nonce to said server.

21. (Original) The system as described in claim 20 and further comprising:

computer code coupled to said server operable to confirm the value of said
returned_nonce at said server.
